Statistically-Hiding Commitment from Any One-Way Function

Iftach Haitner
Dept. of Computer Science and Applied Math.,
Weizmann Institute of Science
Rehovot 76100, Israel
iftach.haitner@weizmann.ac.il

Omer Reingold*
Dept. of Computer Science and Applied Math.,
Weizmann Institute of Science
Rehovot 76100, Israel
omer.reingold@weizmann.ac.il

ABSTRACT

We give a construction of statistically-hiding commitment schemes (ones where the hiding property holds information theoretically), based on the minimal cryptographic assumption that one-way functions exist. Our construction employs two-phase commitment schemes, recently constructed by Nguyen, Ong and Vadhan (FOCS '06), and universal one-way hash functions introduced and constructed by Naor and Yung (STOC '89) and Rompel (STOC '90).

Categories and Subject Descriptors

F.1.2 [**Modes of Computation**]: Interactive and reactive computation

General Terms

Theory

Keywords

Cryptography, One-way functions, Statistically hiding and computationally binding commitment.

1. INTRODUCTION

A commitment scheme defines a two-stage interactive protocol between a sender $\mathcal{S}$ and a receiver $\mathcal{R}$; informally, after the *commit stage*, $\mathcal{S}$ is bound to (at most) one value, which stays hidden from $\mathcal{R}$, and in the *reveal stage* $\mathcal{R}$ learns this value. The two security properties hinted at in this informal description are known as *binding* (namely, that $\mathcal{S}$ is bound to at most one value after the commit stage) and *hiding* (namely, that $\mathcal{R}$ does not learn the value to which $\mathcal{S}$ commits before the reveal stage). In a statistically-hiding computationally-binding commitment scheme (for short, statistical commitment) the hiding property holds *even against all-powerful receivers* (i.e., hiding holds information-theoretically), while the binding property is required to hold only for polynomially-bounded senders.

Statistical commitment schemes can be used as a building block in constructions of statistical zero-knowledge arguments [2, 14] and certain coin-tossing protocols [12]. It therefore implies, via standard reduction, a way to transform a large class of protocols that are secure assuming an all powerful honest-but-curious party, into one that is secure even when this party maliciously deviates from the protocol. More generally, when used within protocols in which certain commitments are never revealed, statistical commitments have the following advantage over computationally-hiding commitment schemes: in such a scenario, it needs only be infeasible to violate the binding property *during the period of time the protocol is run*, whereas the committed values will remain hidden *forever* (i.e., regardless of how much time the receiver invests after completion of the protocol).

Perfectly-hiding[1] commitment schemes were first shown to exist based on specific number-theoretic assumptions [1, 2] or, more generally, based on any collection of claw-free permutations [7] with an efficiently-recognizable index set [6]. Statistical commitment schemes can also be constructed from collision-resistant hash functions [4, 15]. Naor et al. [14] showed a construction of a perfectly-hiding commitment scheme based on any one-way permutation. Haitner et. al. [8] make progress by constructing statistical commitment based on regular one-way functions and also on the so called approximable-size one-way functions.

In their recent breakthrough result, Nguyen et al. [16] show how to construct statistical zero-knowledge arguments for NP based on any one-way function. The question of whether one-way functions imply statistical commitments, however, was left open.

We mention that the complementary notion of commitment schemes, where the hiding is computational and the binding holds even w.r.t. an all powerful sender, was already known to be implied by the existence of one-way functions [9, 13].

*Research supported by grant no. 1300/05 from the Israel Science Foundation.

STOC'07, June 11–13, 2007, San Diego, California, USA.

[1]Very informally, in a statistically-hiding commitment scheme the receiver learns only a negligible amount of information about the sender's committed value, whereas in a perfectly-hiding commitment scheme the receiver learns *nothing*. Note that any perfectly-hiding scheme is trivially also statistically hiding.

1.1 Our result

Our main result is that the existence of one-way functions is a sufficient condition for the existence of statistical commitment. Namely, we prove the following theorem.

THEOREM 1.1. *Assuming that one-way functions exist, then there exists a statistically-hiding computationally-binding commitment.*

By Impagliazzo and Luby [10], the existence of statistical commitment schemes implies the existence of one-way functions and thus the above result is tight.

1.2 Our technique

Our protocol combines, in a sense, the following two cryptographic primitives: two-phase commitment schemes recently presented by Nguyen et al. [16] (extending a similar notion given in [17]) and universal one-way hash functions presented by Naor and Yung [15]. Following is an informal description of the primitives (a formal definition appears in Section 2).

Universal one-way hash functions Universal one-way hash functions are a relaxation of the notion of collision-resistant hash functions. A family of compressing hash functions is universal one-way if no efficient algorithm succeeds in the following game with more than negligible probability. The algorithm should first announce a value x. Then, on a uniformly selected hash function f (given to the algorithm *after* it announces x), it should find $x' \neq x$ such that $f(x') = f(x)$.

Rompel [18] shows that the existence of one-way functions implies the existence of universal one-way hash functions, this result was recently rewritten by Katz and Koo [11], adding missing details and fixing some errors.

Two-phase commitments In a two-phase commitment scheme, the sender and the receiver interact in two consecutive phases. In each phase they carry out a commitment protocol (the commit stage and the reveal stage). The transcript of the first phase is used as input for the second-phase commitment. A two-phase commitment is statistically hiding, if before each of the reveal stages the receiver has no information about the committed value. A two-phase commitment is $\binom{2}{1}$-binding, if the sender cannot cheat both in the first phase and in the second phase. Specifically, after the first-phase commit, there is a *single* value such that if the sender decommits to any other value, then the second commitment is guaranteed to be binding (in the standard sense).

Nguyen et al. [16] prove that the existence of one-way functions implies some non-uniform version of two-phase commitment schemes.

The construction idea.

We would like to use two-phase commitment schemes to construct a (standard) statistical commitment. A naive attempt to design the commitment scheme may go as follows: First, the sender commits to some random string x using the first-phase commit stage. Then, the receiver flips a coin $phase \in \{\mathsf{first}, \mathsf{second}\}$, if $phase = \mathsf{first}$ then the first-phase commitment is used as the commitment (e.g., the sender sends to the receiver the exclusive or of its secret with the random string). Otherwise ($phase = \mathsf{second}$), the two parties execute the first-phase reveal stage and if successful (i.e., the receiver does not reject), they use the second-phase commitment (invoked with the transcript of the first-phase as input) as the commitment.

The intuition is that since the two-phase commitment is $\binom{2}{1}$-binding, the sender cannot cheat in both phases together and thus the receiver would catch a cheating sender with probability half. The problem is, however, that the sender can decide in which commitment he likes to cheat *after* knowing the value of *phase*. Hence, the sender can cheat successfully in both cases without violating the $\binom{2}{1}$-binding of the underlying protocol.

Our key idea is to use universal one-way hash functions in order to force the sender to decide in which phase it is about to cheat *before* knowing the value of *phase*. Our actual implementation is as follows: After the first-phase commit stage, the receiver selects a random (universal one-way) hash function f and the sender sends him back $y = f(x)$. The protocol proceeds essentially as the naive protocol above, where any time the first-phase reveal stage is executed in the naive protocol revealing the value x' (either in the commit-stage for $phase = \mathsf{first}$ or in the reveal stage for $phase = \mathsf{second}$), the receiver also verifies that $f(x') = y$.

Assuming that the hash function, f, is "compressing enough", the string x (committed to in the first-phase commitment) remains sufficiently hidden even $f(x)$ is sent to $\mathcal{R}$ (in the new variant of the protocol). Thus, in the case that $phase = \mathsf{first}$, the string x can still be used to statistically hide the sender's secret (assuming it is sufficiently shorter than x). To show the statistical hiding in the complementary case when $phase = \mathsf{second}$, it is sufficient to note that sending $f(x)$, does not compromise the hiding property of the second-phase commitment. All in all, the protocol is statistically hiding for both choices of *phase* and thus it is statistically hiding.

To argue about the binding of the protocol, recall that the $\binom{2}{1}$-binding of the two-phase commitment scheme informally states that after the first-phase commit stage, there exists a *single* value $\widetilde{x}$ that allows the sender to cheat in the second-phase commitment. Now, if the sender sends y such that $f(\widetilde{x}) = y$, then in order to cheat in the case $phase = \mathsf{first}$, it will have to open the first-phase commitment to a value $x' \neq \widetilde{x}$ such that $f(x') = y = f(\widetilde{x})$. This would imply the breaking of the universal one-way hash functions. On the other hand, if $f(\widetilde{x}) \neq y$, then in the case $phase = \mathsf{second}$ the sender is forced to open the first-phase commitment to a value different than $\widetilde{x}$. This guarantees that the sender cannot cheat in the second-phase commitment and thus in this case our protocol is binding. In conclusion, since y is sent before *phase* is chosen, we are guaranteed that our protocol is weakly-binding (since intuitively there always exists a choice of *phase* that prevent the sender from cheating). We complete the construction by amplifying the above protocol into a full-fledged statistical commitment scheme using standard techniques.

2. PRELIMINARIES

2.1 Notation

We denote the i^{th} bit of a string x by $x[i]$. We denote the exclusive or of the bits x and y by $x \oplus y$. For $k \in \mathbb{N}$, we denote by $[k]$ the set $\{1, \ldots, k\}$. Given a set L, we denote by $x \leftarrow L$ the experiment in which x is uniformly chosen from L. The statistical distance of two distributions P and Q over Ω, denoted $SD(P, Q)$, is defined as

$$SD(P,Q) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x \in \Omega} \left| \Pr_P(x) - \Pr_Q(x) \right|.$$

Given two interactive Turing machines (ITM) A and B, we denote the protocol they define by (A, B) and denote the following experiment by $(o_A \mid o_B) \leftarrow \langle A(i_A), B(i_B) \rangle$: The protocol (A, B) is invoked with inputs i_A and i_B and the outputs of the parties are assigned to o_A and o_B respectively.

2.2 Pairwise independent hash functions

DEFINITION 2.1 (PAIRWISE INDEPENDENT HASH FUNCTIONS). *Let $\mathcal{H}$ be a family of functions mapping strings of length $\ell(n)$ to strings of length $m(n)$. We say that $\mathcal{H}$ is an* efficient family of pairwise independent hash functions *(following [3]) if the following hold:* [2]

Samplable. *$\mathcal{H}$ is polynomially samplable (in n).*

Efficient. *There exists a polynomial-time algorithm that given $x \in \{0,1\}^{\ell(n)}$ and a description of $h \in \mathcal{H}$ outputs $h(x)$.*

Pairwise independence. *For every distinct $x_1, x_2 \in \{0,1\}^{\ell(n)}$ and every $y_1, y_2 \in \{0,1\}^{m(n)}$, we have:*

$$\Pr_{h \leftarrow \mathcal{H}}[h(x_1) = y_1 \bigwedge h(x_2) = y_2] = 2^{-2m(n)}.$$

It is well known ([3]) that there exists an efficient family of pairwise-independent hash functions for every choice of ℓ and m whose elements description size is $\mathcal{O}(\max\{\ell(n), m(n)\})$.

In this paper we focus on Boolean families of hash functions (i.e., $m(n) = 1$). The following standard lemma (see for example, [5, Lemma 4.3.1]) states that a random pairwise independent hash function partitions a given set into (almost) equal size subsets.

LEMMA 2.2. *Let $\mathcal{H}$ be a family of Boolean pairwise independent hash functions defined over strings of length $\ell(n)$ and let $L \subseteq \{0,1\}^{\ell(n)}$. Then for every $\delta > 0$*

$$\Pr_{h \leftarrow \mathcal{H}}\left[\left| \left| h^{-1}(1) \cap L \right| - \left| h^{-1}(0) \cap L \right| \right| > \delta \cdot |L| \right] < \tfrac{4}{\delta^2 \cdot |L|}.$$

[2]The first two properties, regarding the efficiency of the family, implicitly assume an ensemble of families (one family for every value of n). For simplify of presentation, we only refer to a single family.

2.3 Universal one-way hash functions

DEFINITION 2.3 (UNIVERSAL ONE-WAY HASH FUNCTIONS). *Let $\mathcal{F}$ be a family of functions mapping strings of length $\ell(n)$ to strings of length $m(n)$. We say that $\mathcal{F}$ is a family of* universal one-way hash functions *(following [15]) if the following hold:* [3]

Samplable. *$\mathcal{F}$ is polynomially samplable (in n).*

Efficient. *There exists a polynomial-time algorithm that given $x \in \{0,1\}^{\ell(n)}$ and a description of $f \in \mathcal{F}$ outputs $f(x)$.*

Compression. *$m(n) < \ell(n)$.*

Hardness. *For all* PPT *A and $x \in \{0,1\}^{\ell(n)}$ the following is negligible in n:*

$$\Pr[(x, \mathsf{state}) \leftarrow A(1^n), f \leftarrow \mathcal{F}, x' \leftarrow A(x, \mathsf{state}, f) : x' \neq x \bigwedge f(x') = f(x)].$$

By [18] (full proof is given in [11]), it follows that assuming the existence of a one-way function, there exists a family of universal one-way hash functions for some polynomial $\ell(n) \geq n$. [4] Following [15, Lemma 2.1], we have that the latter construction implies a construction with $m(n) \leq \frac{1}{2}\ell(n)$. Therefore, we have the following theorem.

THEOREM 2.4. *([11, 15, 18]) If one way functions exist, then for some positive polynomial $\ell(n) \geq n$ there exists a family of universal one-way hash functions mapping strings of length $\ell(n)$ to strings of length $m(n) \leq \ell(n)/2$.*

2.4 Commitment schemes

In this paper we focus on bit-commitment schemes (i.e., the committed string is a single bit). Bit-commitment schemes imply, via standard reductions, commitment schemes of any (polynomial) length.

An interactive bit-commitment scheme $(\mathcal{S}, \mathcal{R})$, with security parameter n, consists of two probabilistic polynomial-time interactive protocols: $(\mathcal{S}_c, \mathcal{R}_c)$, the commit stage, and $(\mathcal{S}_r, \mathcal{R}_r)$, the reveal stage. We note that in all the constructions of this paper, the reveal stage will always be non interactive, consisting of a single message from the sender to the receiver. Throughout, both parties receive the security parameter 1^n as an input.

1. In the commit stage: $\mathcal{S}_c$ receives a private input $b \in \{0,1\}$. At the end, $\mathcal{S}_c$ *locally* outputs some private information prvt and $\mathcal{R}_c$ outputs some public information pub.

2. In the reveal stage: $\mathcal{S}_r$ and $\mathcal{R}_r$ receive a common input pub and a bit b and $\mathcal{S}_r$ receives a private input prvt. At the end, $\mathcal{R}_r$ accepts or rejects.

[3]We use the same convention as in Definition 2.1.

[4]The Hardness property of Definition 2.3 is somewhat stronger than the one given in [11] (and somewhat weaker than the original definition in [15]). The strengthening is in allowing A to transfer additional information, i.e., state, between the selection of x and finding the collision. We note that the proof in [11] holds also w.r.t. to our stronger definition (and even w.r.t. the original definition of [15]).

We make the following correctness requirement: For all n, all $b \in \{0,1\}$, and every pair $(\mathsf{prvt}, \mathsf{pub})$ that may be output by $\langle \mathcal{S}_c(1^n, b), \mathcal{R}_c(1^n)\rangle$, it is the case that $\mathcal{R}_r$ accepts in the interaction $\langle \mathcal{S}_r(1^n, \mathsf{prvt}, \mathsf{pub}, b), \mathcal{R}_r(1^n, \mathsf{pub}, b)\rangle$.

The security of a commitment scheme can be defined in two complementary ways, protecting against either an all-powerful sender or an all-powerful receiver. In this paper, we are interested in the case of statistical commitment (i.e., the latter case).

DEFINITION 2.5 (STATISTICALLY HIDING). *A bit-commitment scheme $(\mathcal{S}, \mathcal{R})$ is ρ-*hiding *(for ρ a function of n) if the following holds: Given an* ITM *$\mathcal{R}^*$, let $\mathsf{view}_{\langle \mathcal{S}_c(b), \mathcal{R}^*\rangle}(n)$ denote the distribution on the view of $\mathcal{R}^*$ when interacting with $\mathcal{S}_c(1^n, b)$ (this view simply consists of $\mathcal{R}^*$'s random-coins and the sequence of messages it receives from $\mathcal{S}_c$), where this distribution is taken over the random coins of $\mathcal{S}_c$ and $\mathcal{R}^*$. Then we require that for any (even all-powerful) $\mathcal{R}^*$ the two ensembles $\{\mathsf{view}_{\langle \mathcal{S}_c(0), \mathcal{R}^*\rangle}(n)\}$ and $\{\mathsf{view}_{\langle \mathcal{S}_c(1), \mathcal{R}^*\rangle}(n)\}$ have statistical difference at most ρ.*

We say that a scheme is *statistically hiding* if it is ρ-hiding for negligible ρ. A 0-hiding scheme is called *perfectly hiding*.

DEFINITION 2.6 (BINDING-BREAK). *Let $(\mathcal{S}, \mathcal{R})$ be a bit commitment protocol and let $\mathcal{S}^* = (\mathcal{S}_c^*, \mathcal{S}_r^*)$ be an algorithm that is trying to break the binding of this protocol. For any possible values of the commit stage, $\mathsf{outs} = (\mathsf{prvt}, \mathsf{pub})$, we define the function $\mathsf{BindBreak}^{\mathcal{S}_r^*, \mathcal{R}_r}(\mathsf{outs}) \stackrel{def}{=} \min_{b\in\{0,1\}} \Pr[\langle \mathcal{S}_r^*(\mathsf{outs}, b), \mathcal{R}_r(\mathsf{pub}, b)\rangle = \mathtt{Accept}]$.*

DEFINITION 2.7 (COMPUTATIONALLY BINDING). *A bit-commitment scheme $(\mathcal{S}, \mathcal{R})$ is ρ-binding (for ρ a function of n), if for all* PPT *$\mathcal{S}^*$ and any positive polynomial p, the following holds for large enough n:*

$$\Pr_{\mathsf{outs} \leftarrow \langle \mathcal{S}_c^*(1^n), \mathcal{R}_c(1^n)\rangle}[\mathsf{BindBreak}^{\mathcal{S}_r^*, \mathcal{R}_r}(\mathsf{outs}) > \frac{1}{p(n)}] < \rho(n).$$

Note that in the above, assuming that $\mathcal{S}^*$ consists of two separate algorithms is without loss of generality, since any information that $\mathcal{S}^*$ passes between the two stages can be encoded into its private output. We say that a scheme is *computationally binding* if it is ρ-binding for negligible ρ. The following amplifications are standard (see for example [8]).

PROPOSITION 2.8. *There exists an efficient procedure that given polynomially many bit-commitment schemes which are all computationally binding and at least one of them is statistically hiding, outputs a computationally-binding statistically-hiding bit-commitment scheme.*

PROPOSITION 2.9. *There exists an efficient procedure that given a $(1-\delta)$-binding bit-commitment scheme for some noticeable δ, outputs a computationally-binding bit-commitment scheme, which is statistically hiding if the given bit-commitment scheme is.*

2.5 Two-phase commitments

The following definitions are taken from [16].

DEFINITION 2.10 (TWO-PHASE COMMITMENTS). *A* two-phase commitment scheme *$(\mathcal{S}, \mathcal{R})$, with security parameter n and message lengths $(k_1, k_2) = (k_1(n), k_2(n))$, consists of four probabilistic polynomial-time interactive protocols: $(\mathcal{S}_c^1, \mathcal{R}_c^1)$ the first commit stage, $(\mathcal{S}_r^1, \mathcal{R}_r^1)$ the first reveal stage, $(\mathcal{S}_c^2, \mathcal{R}_c^2)$ the second commit stage, and $(\mathcal{S}_r^2, \mathcal{R}_r^2)$ the second reveal stage. Throughout, both parties receive the security parameter 1^n as input.*

1. *In the first commit stage, $\mathcal{S}_c^1$ receives a private input $\sigma^{(1)} \in \{0,1\}^{k_1}$. At the end, $\mathcal{S}_c^1$* locally *outputs some private information prvt^1 and $\mathcal{R}_c^1$ outputs some public string pub^1.*
2. *In the first reveal stage, $\mathcal{S}_r^1$ and $\mathcal{R}_r^1$ receive as common input pub^1 and a string $\sigma^{(1)} \in \{0,1\}^{k_1}$ and $\mathcal{S}_r^1$ receives as private input prvt^1. Let trans be the transcript of the first commit stage and the first reveal stage and includes $\mathcal{R}_r^1$'s decision to accept or reject.*
3. *In the second commit stage, $\mathcal{S}_c^2$ and $\mathcal{R}_c^2$ both receive the common input trans, and $\mathcal{S}_c^2$ receives a private input $\sigma^{(2)} \in \{0,1\}^{k_2}$ and prvt^1. At the end, $\mathcal{R}_c^2$ outputs some public string pub^2.*
4. *In the second reveal stage, $\mathcal{S}_r^2$ and $\mathcal{R}_r^2$ receive as common input pub^2 and a string $\sigma^{(2)} \in \{0,1\}^{k_2}$, and $\mathcal{S}_r^2$ receives as private input prvt^1. At the end, $\mathcal{R}_r^2$ accepts or rejects.*

As for standard commitment schemes, the security of the sender is defined in terms of a hiding property. Loosely speaking, the hiding property for a two-phase commitment scheme says that *both* commit phases are hiding. Note that since the phases are run sequentially, the hiding property for the second commit stage is required to hold even given the receiver's view of the first stage.

DEFINITION 2.11 (STATISTICALLY HIDING). *A two-phase commitment scheme $(\mathcal{S}, \mathcal{R})$, with security parameter n and message lengths $(k_1, k_2) = (k_1(n), k_2(n))$, is* statistically hiding *if the following hold: Given an* ITM *$\mathcal{R}^*$ and some value of $\sigma^{(1)}$, let $\mathsf{view}_{\langle \mathcal{S}_c^1(\sigma^{(1)}), \mathcal{R}^*\rangle}(n)$ denote the distribution on the view of $\mathcal{R}^*(1^n)$ when interacting with $\mathcal{S}_c^1(1^n, \sigma^{(1)})$. Similarly, for some values of $\sigma^{(2)}$, prvt^1 and trans, let $\mathsf{view}_{\langle \mathcal{S}_c^2(\sigma^{(2)}, \mathsf{prvt}^1), \mathcal{R}^*\rangle}(\mathsf{trans})$ denote the distribution on the view of $\mathcal{R}^*(\mathsf{trans})$ when interacting with $\mathcal{S}_c^2(\sigma^{(2)}, \mathsf{prvt}^1, \mathsf{trans})$. We require that for any (even all-powerful) $\mathcal{R}^*$,*

1. *The views of $\mathcal{R}^*$ when interacting with the sender in the first phase on any two messages are statistically indistinguishable. That is, for all $\sigma^{(1)}, \widetilde{\sigma}^{(1)} \in \{0,1\}^{k_1}$, $\mathsf{view}_{\langle \mathcal{S}_c^1(\sigma^{(1)}), \mathcal{R}^*\rangle}(n)$ is statistically indistinguishable to $\mathsf{view}_{\langle \mathcal{S}_c^1(\widetilde{\sigma}^{(1)}), \mathcal{R}^*\rangle}(n)$.*
2. *The views of $\mathcal{R}^*$ when interacting with the sender in the second phase are statistically indistinguishable no matter what the sender committed to in the first phase. That is, for all $\sigma^{(1)} \in \{0,1\}^{k_1}$ and $\sigma^{(2)}, \widetilde{\sigma}^{(2)} \in \{0,1\}^{k_2}$, $\mathsf{view}_{\langle \mathcal{S}_c^2(\sigma^{(2)}, \mathsf{prvt}^1), \mathcal{R}^*\rangle}(\mathsf{trans})$ is statistically indistinguishable to $\mathsf{view}_{\langle \mathcal{S}_c^2(\widetilde{\sigma}^{(2)}, \mathsf{prvt}^1), \mathcal{R}^*\rangle}(\mathsf{trans})$,*

where prvt^1 *is the private output of* $\mathcal{S}_c^1$ *in the first-phase commit stage and* $\mathsf{trans} = \mathsf{transcript}\langle \mathcal{S}^1(1^n, \sigma^{(1)}), \mathcal{R}^*(1^n)\rangle$.

We stress that the second condition of the above hiding definition (Definition 2.11) requires that the view of receiver in the second phase be indistinguishable for any two messages even given the transcript of the first phase, $\mathsf{trans} = \mathsf{transcript}\langle \mathcal{S}^1(1^n, \sigma^{(1)}), \mathcal{R}^*(1^n)\rangle$.

Loosely speaking, the binding property says that *at least* one of the two commit phases is (computationally) binding. In other words, for every polynomial-time sender $\mathcal{S}^*$, there is at most one "bad" phase $j \in \{1, 2\}$ such that given the common output pub^j, $\mathcal{S}^*$ can open pub^j successfully both as $\sigma^{(j)}$ and $\widetilde{\sigma}^{(j)} \neq \sigma^{(j)}$ with non-negligible probability. Actually, we allow this bad phase to be determined dynamically by $\mathcal{S}^*$. Moreover, the second phase is *statistically* binding if the sender breaks the first phase. [5]

DEFINITION 2.12 ($\binom{2}{1}$-BINDING). *A two-phase commitment scheme* $(\mathcal{S}, \mathcal{R})$*, with security parameter* n *and message lengths* $(k_1, k_2) = (k_1(n), k_2(n))$*, is* computationally $\binom{2}{1}$-binding *if there exists a set* $\mathcal{B}$ *of first-phase transcripts and a negligible function* ε *such that:*

1. *For every (even unbounded) sender* $\mathcal{S}^*$*, the first-phase transcripts in* $\mathcal{B}$ *make the second phase statistically binding, i.e.,* $\forall$ ITM S^*, $\forall \mathsf{trans} \in \mathcal{B}$*, with probability at least* $1 - \varepsilon(n)$ *over* pub^2*, the output of* $\mathcal{R}_c^2$ *in* $\langle \mathcal{S}^*(\mathsf{prvt}^1, \mathsf{trans}), R_c^2(\mathsf{trans})\rangle$*, there is at most one value* $\sigma^{(2)} \in \{0,1\}^{k_2}$ *such that* $\langle \mathcal{S}^*(\mathsf{prvt}^1, \mathsf{pub}^2, \sigma^{(2)}), R_r^2(\mathsf{pub}^2, \sigma^{(2)})\rangle = \mathtt{Accept}$.
2. *Any* PPT $\mathcal{S}^*$ *succeeds in the following game with probability at most* $\varepsilon(n)$ *for all sufficiently large* n*:*
   (a) $\mathcal{S}^*$ *and* $\mathcal{R}_c^1$ *interact and* $\mathcal{R}_c^1$ *outputs* pub^1*. Let* trans^1 *be the transcript of the interaction.*
   (b) $\mathcal{S}^*$ *outputs two full transcripts* trans *and* $\widetilde{\mathsf{trans}}$ *of* both *phases with the following three properties:*
      - *Transcripts* trans *and* $\widetilde{\mathsf{trans}}$ *both start with prefix* trans^1.
      - *The transcript* trans *contains a successful opening of* pub^1 *to the value* $\sigma^{(1)} \in \{0,1\}^{k_1}$ *using a first-phase transcript not in* $\mathcal{B}$*, and* $\mathcal{R}_r^1$ *and* $\mathcal{R}_r^2$ *both accept in* trans.
      - *The transcript* $\widetilde{\mathsf{trans}}$ *contains a successful opening of* pub^1 *to the value* $\widetilde{\sigma}^{(1)} \in \{0,1\}^{k_1}$ *using a first-phase transcript not in* $\mathcal{B}$*, and* $\mathcal{R}_r^1$ *and* $\mathcal{R}_r^2$ *both accept in* $\widetilde{\mathsf{trans}}$.
   (c) $\mathcal{S}^*$ *succeeds if all of the above conditions hold and* $\sigma^{(1)} \neq \widetilde{\sigma}^{(1)}$.

[5] In this paper, we do not use the fact that the second phase is statistically binding and not merely computationally binding.

THEOREM 2.13. *([16, Theorem 7.10]) If one way functions exist, then there exists an efficient procedure that on security parameter* n*, outputs a collection of public-coin two-phase commitment schemes* $Com_1, \ldots, Com_m$ *for* $m = \mathsf{poly}(n)$ *such that:*

- *There exists an index* i *such that the scheme* Com_i *is statistically hiding.* [6]
- *For every index* j*, scheme* Com_j *is* $\binom{2}{1}$*-binding.*

REMARK 2.14. *While not stated explicitly in [16], the proof of Theorem 2.13 yields that the message lengths of* $Com_1, \ldots, Com_m$*, which appear in the theorem, can be chosen to be any positive polynomials.*

3. THE CONSTRUCTION

Given a two-phase commitment scheme and a family of universal one-way hash functions, we construct a bit-commitment scheme such that the following holds: The scheme is statistically hiding whenever the two-phase commitment scheme is statistically hiding and the scheme is *weakly* binding whenever the two-phase commitment scheme is $\binom{2}{1}$-binding. Thus, assuming that one-way functions exist, the existence of a polynomial set of weakly-binding bit-commitment schemes where at least one of them is statistically hiding follows by Theorem 2.4 and Theorem 2.13. Finally, we use standard reductions to amplify the latter set of commitment schemes into a full-fledged statistical commitment scheme.

3.1 Main reduction

In this section we construct a bit-commitment scheme with the following properties: The scheme is statistically hiding whenever the two-phase commitment is statistically hiding and the scheme is weakly binding whenever the two-phase commitment is $\binom{2}{1}$-binding.

CONSTRUCTION 3.1 (THE BASIC SCHEME). *Let* $\mathcal{F}$ *be a family of universal one-way hash functions mapping strings of length* $\ell(n)$ *to strings of length* $m(n) \leq \frac{1}{2}\ell(n)$*, let* $\mathcal{H}$ *be a family of Boolean pairwise independent hash functions defined over strings of length* $\ell(n)$ *and finally let* $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ *be a two-phase commitment scheme with message lengths* $(\ell(n), 1)$*. We define the bit-commitment protocol* $(\mathcal{S}, \mathcal{R})$ *as follows:*

[6] This property holds, regardless of whether the one-way function for which the scheme is based on is one-way or not.

Commit stage:

Common input: 1^n.
Sender's private input: $b \in \{0,1\}$.

1. $\mathcal{S}_c$ *chooses uniformly at random* $z \in \{0,1\}^{\ell(n)}$.
2. $(\mathcal{S}_c, \mathcal{R}_c)$ *run* $\langle \widetilde{\mathcal{S}}_c^1(z), \widetilde{\mathcal{R}}_c^1(1^n)\rangle$, *with* $\mathcal{S}_c$ *and* $\mathcal{R}_c$ *acting as* $\widetilde{\mathcal{S}}_c^1$ *and* $\widetilde{\mathcal{R}}_c^1$ *respectively.*

   Let pub^1 *be the public output and let* prvt^1 *be the private output of* $\widetilde{\mathcal{S}}_c^1$ *in the above interaction.*
3. $\mathcal{R}_c$ *chooses uniformly at random* $f \in \mathcal{F}$ *and sends it to* $\mathcal{S}$.
4. $\mathcal{S}_c$ *sends* $y = f(z)$ *back to* $\mathcal{R}$.
5. $\mathcal{R}_c$ *chooses a random value* $phase \in \{\mathsf{first}, \mathsf{second}\}$.

   If $phase = \mathsf{first}$, **// Basing the commitment on the hardness of** $\mathcal{F}$**.**

   (a) $\mathcal{S}_c$ *chooses uniformly at random* $h \in \mathcal{H}$ *and sends* h *and* $c = b \oplus h(z)$ *to* $\mathcal{R}_c$.

   (b) $\mathcal{R}_c$ *outputs* $\mathsf{pub} = (\mathsf{first}, f, y, h, c)$.

   (c) $\mathcal{S}_c$ *locally outputs* $\mathsf{prvt} = z$.

   Otherwise (i.e., $phase = \mathsf{second}$*),* **// Basing the commitment on the second phase commitment.**

   $\mathcal{S}_c$ *sends* z *to* $\mathcal{R}_c$ *and* $(\mathcal{S}_c, \mathcal{R}_c)$ *run* $\langle \widetilde{\mathcal{S}}_r^1(\mathsf{prvt}^1, \mathsf{pub}^1, z), \widetilde{\mathcal{R}}_r^1(\mathsf{pub}^1), z)\rangle$, *with* $\mathcal{S}_c$ *and* $\mathcal{R}_c$ *acting as* $\widetilde{\mathcal{S}}_c^1$ *and* $\widetilde{\mathcal{R}}_c^1$ *respectively. Let* trans *be the transcript of the above interaction.*

   If $\widetilde{\mathcal{R}}_c^r$ *rejects, then* $\mathcal{R}_c$ *outputs* $\perp$ *(i.e., it will be impossible to decommit this interaction). Otherwise,*

   (a) $(\mathcal{S}_c, \mathcal{R}_c)$ *run* $\langle \widetilde{\mathcal{S}}_c^2(b, \mathsf{prvt}^1, \mathsf{trans}), \widetilde{\mathcal{R}}_c^2(\mathsf{trans})\rangle$, *with* $\mathcal{S}_c$ *and* $\mathcal{R}_c$ *acting as* $\widetilde{\mathcal{S}}_c^2$ *and* $\widetilde{\mathcal{R}}_c^2$ *respectively.*

   Let pub^2 *be the public output in the above interaction.*

   (b) $\mathcal{S}_c$ *locally outputs* $\mathsf{prvt} = \mathsf{prvt}^1$ *and* $\mathcal{R}_c$ *outputs* $\mathsf{pub} = (\mathsf{second}, \mathsf{pub}^2)$.

Reveal stage:

In case $phase = \mathsf{first}$**,**
Common input: 1^n, $b \in \{0,1\}$ *and* $\mathsf{pub} = (\mathsf{first}, f, y, h, c)$.
Sender's private input: $\mathsf{prvt} = z$.

$\mathcal{S}_r$ *sends* z *to* $\mathcal{R}_r$.

If $f(z) \neq y$ *or* $c \oplus h(z) \neq b$, *then* $\mathcal{R}_r$ *outputs* `Reject`. *Otherwise,* $\mathcal{R}_r$ *outputs* `Accept`.

In case $phase = \mathsf{second}$**,**
Common input: 1^n, $b \in \{0,1\}$ *and* $\mathsf{pub} = (\mathsf{second}, \mathsf{pub}^2)$.
Sender's private input: $\mathsf{prvt} = \mathsf{prvt}^1$.

$(\mathcal{S}_r, \mathcal{R}_r)$ *run* $\langle \widetilde{\mathcal{S}}_r^2(\mathsf{prvt}^1, \mathsf{pub}^2, b), \widetilde{\mathcal{R}}_r^2(\mathsf{pub}^2, b)\rangle$, *with* $\mathcal{S}_r$ *and* $\mathcal{R}_r$ *acting as* $\widetilde{\mathcal{S}}_r^2$ *and* $\widetilde{\mathcal{R}}_r^2$ *respectively.*
$\mathcal{R}_r$ *outputs the same output as* $\widetilde{\mathcal{R}}_r^2$ *does in the above interaction.*

The correctness of the above commitment scheme is evident given that the underlying two-phase commitment is correct. In Section 3.1.1, we prove that above scheme is statistically hiding whenever the underlying two-phase commitment is hiding. In Section 3.1.2, we prove that if $\mathcal{F}$ is a family of universal one-way hash functions and the underlying two-phase commitment is $\binom{2}{1}$-binding, then the above scheme is weakly binding.

REMARK 3.2. *We note that by changing slightly the protocol of Construction 3.1, we could directly get a weakly-binding statistically-hiding commitment scheme for* any polynomial length *(rather than for a single bit). Since the proof of the current version is somewhat simpler, and since the transformation from bit-commitment scheme to commitment scheme of any (polynomial) length bit-strings is standard, we chose to present the above version.*

3.1.1 The scheme is statistically hiding

LEMMA 3.3. *If* $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ *is statistically hiding, then* $(\mathcal{S}, \mathcal{R})$ *is statistically hiding.*

PROOF. Assuming that $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is statistically hiding, then the (statistical) hiding in the case that $phase = \mathsf{second}$ is evident. That is, by the hiding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$, no information about b has leaked to the receiver. Note that the receiver also gets the values of f and $f(z)$, but this information could be generated from z and thus it reveals no additional information about b.

In the complementary case ($phase = \mathsf{first}$) the situation is a bit more involved. Essentially, the only information that the receiver obtains about b is $y = f(z)$ and $c = b \oplus h(z)$. Since f is condensing and by the pairwise independence of $\mathcal{H}$, it is easy to see that with overwhelming probability (y, c) contains only negligible information about b and thus the protocol is statistically hiding. Let us turn to the formal proof. Let $(\mathcal{S}', \mathcal{R}')$ be the same protocol as $(\mathcal{S}, \mathcal{R})$, but where in Line (2) of the commit stage, the first-phase commit of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$, is always executed with $\widetilde{\mathcal{S}}_c^1$'s input set to $0^{\ell(n)}$ (instead of z) and *phase* is always set to first. Since $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is statistically hiding, $(\mathcal{S}', \mathcal{R}')$ is statistically hiding if and only if $(\mathcal{S}, \mathcal{R})$ is. Otherwise, one could have designed a statistical test that distinguishes a commitment to $0^{\ell(n)}$ from a commitment to a random z (that is known to the test), which contradicts the statistical hiding of the first phase of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$. Hence, for the following discussion we concentrate on the hiding property of the protocol $(\mathcal{S}'', \mathcal{R}'')$, where Line (2) is not executed at all (it is obvious that $(\mathcal{S}'', \mathcal{R}'')$ is statistically hiding if and only if $(\mathcal{S}', \mathcal{R}')$ is).

Let us fix a deterministic ITM $\mathcal{R}^*$ that interacts with $\mathcal{S}_c''$ in the commit stage of $(\mathcal{S}'', \mathcal{R}'')$, note that since we allow $\mathcal{R}^*$ to be unbounded, assuming that $\mathcal{R}^*$ is deterministic is without loss of generality. For a given value of n, it follows that since $\mathcal{R}^*$ is deterministic and it sends the hash function f as the first message of the interaction, f is the same in all interactions. We denote this value of f by f^*. The view of $\mathcal{R}^*$ when interacting with $\mathcal{S}_c''$ consists of the values of $y = f^*(z)$, h and $c = b \oplus h(z)$. Note that the only difference between a commitment to one and a commitment to zero is the value of c. Let v be a possible view of $\mathcal{R}^*$ in the interaction with $\mathcal{S}_c''$ and let h, y and c be the values of these variables in v. It follows that for both $b \in \{0,1\}$ $Pr[\mathsf{view}_{\langle \mathcal{S}_c''(b), \mathcal{R}^*\rangle}(n) = v] = \frac{1}{|\mathcal{H}|} \cdot \Pr_{z \leftarrow \{0,1\}^{\ell(n)}}[f^*(z) = y] \cdot \Pr_{z \leftarrow \{0,1\}^{\ell(n)}}[b \oplus h(z) = c \mid f^*(z) = y]$. Therefore,

$$
\begin{aligned}
& SD(\mathsf{view}_{\langle \mathcal{S}_c''(0),\mathcal{R}^*\rangle}(n), \mathsf{view}_{\langle \mathcal{S}_c''(1),\mathcal{R}^*\rangle}(n)) \\
= \; & \frac{1}{2}\sum_{v} |\Pr[\mathsf{view}_{\langle \mathcal{S}_c''(0),\mathcal{R}^*\rangle}(n)=v] \\
& - \Pr[\mathsf{view}_{\langle \mathcal{S}_c''(1),\mathcal{R}^*\rangle}(n)=v]| \\
= \; & \frac{1}{2}\cdot\frac{1}{|\mathcal{H}|}\sum_{y,h,c}\Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[f^*(z)=y]\cdot \\
& |\Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[0\oplus h(z)=c \mid f^*(z)=y] \\
- \; & \Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[1\oplus h(z)=c \mid f^*(z)=y]| \\
= \; & \frac{1}{2}\cdot\frac{1}{|\mathcal{H}|}\sum_{y,h}\Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[f^*(z)=y]\cdot \\
& 2\cdot|\Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[h(z)=0 \mid f^*(z)=y] \\
- \; & \Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[h(z)=1 \mid f^*(z)=y]| \\
= \; & \mathop{\mathsf{Ex}}_{z\leftarrow\{0,1\}^{\ell(n)},h\leftarrow\mathcal{H}} \\
& \left[\frac{\left|\left|(f^*)^{-1}(z)\cap h^{-1}(0)\right|-\left|(f^*)^{-1}(z)\cap h^{-1}(1)\right|\right|}{|(f^*)^{-1}(z)|}\right].
\end{aligned}
$$

The proof of Lemma 3.3 is concluded by the following claim and by the pairwise independent of $\mathcal{H}$ (Lemma 2.2).

CLAIM 3.4. *For any $f\in\mathcal{F}$ it holds that $\Pr_{z\leftarrow\{0,1\}^{\ell(n)}}[|f^{-1}(f(z))|\le 2^{\frac{1}{4}\ell(n)}]\le 2^{-\frac{1}{4}\ell(n)}$.*

PROOF. For a given value of $f\in\mathcal{F}$, we say that $y\in\{0,1\}^{m(n)}$ is *light*, if $|f^{-1}(y)|<2^{\frac{1}{4}\ell(n)}$. Clearly, f has at most $2^{m(n)}$ light images and therefore there are at most $2^{\frac{1}{4}\ell(n)}\cdot 2^{m(n)}\le 2^{\frac{3}{4}3\ell(n)}$ elements in $\{0,1\}^{\ell(n)}$ for which $|f^{-1}(f(z))|\le 2^{\ell(n)/4}$. □

3.1.2 The scheme is weakly binding

LEMMA 3.5. *If $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$ is $\binom{2}{1}$-binding and $\mathcal{F}$ is a family of universal one-way hash functions, then $(\mathcal{S},\mathcal{R})$ is $\frac{35}{36}$-binding.*

PROOF. Let $\mathcal{S}^*=(\mathcal{S}_c^*,\mathcal{S}_r^*)$ be an algorithm trying to break the binding of $(\mathcal{S},\mathcal{R})$ and recall $\mathsf{BindBreak}$ from Definition 2.6. Let $d\in\{\mathsf{first},\mathsf{second}\}$ and let p be a positive polynomial, we define $\gamma_d^p(n)\stackrel{\text{def}}{=}\Pr_{\mathsf{outs}\leftarrow\langle\mathcal{S}_c^*(1^n),\mathcal{R}_c(1^n)\rangle}[\mathsf{BindBreak}^{\mathcal{S}_r^*,\mathcal{R}_r}(\mathsf{outs})>\frac{1}{p(n)}|\,phase=d]$ (for ease of reading from now on we omit the superscript $(\mathcal{S}_r^*,\mathcal{R}_r)$ from $\mathsf{BindBreak}$). Namely, $\gamma_d^p(n)$ is the probability that conditioned on $phase=d$, the output of the commit stage enables $\mathcal{S}^*$ to cheat in the reveal stage with noticeable probability. The proof of the Lemma 3.5 follows by the next claim.

CLAIM 3.6. *Let p be a positive polynomial, then for large enough n there exists $d\in\{\mathsf{first},\mathsf{second}\}$ such that $\gamma_d^p(n)<\frac{17}{18}$.*

Therefore, for any positive polynomial p and large enough n, $\Pr_{\mathsf{outs}\leftarrow\langle\mathcal{S}^*(1^n),\mathcal{R}_c(1^n)\rangle}[\mathsf{BindBreak}(\mathsf{outs})>\frac{1}{p(n)}]=\Pr[phase=\mathsf{first}]\cdot\gamma_0^p(n)+\Pr[phase=\mathsf{second}]\cdot\gamma_1^p(n)\le 1-\frac{1}{2}\cdot\frac{1}{18}$ and the proof of Lemma 3.5 follows.

PROOF. (of Claim 3.6) We assume toward a contradiction that the claim does not hold and prove that either the hardness of the universal one-way hash functions or the $\binom{2}{1}$-binding of the underlying two-phase commitment scheme are violated. More formally, let p be a positive polynomial that for infinitely many n's and for both values of $d\in\{\mathsf{first},\mathsf{second}\}$, it holds that $\gamma_d^p(n)\ge\frac{9}{10}$. Assuming that the $\binom{2}{1}$-binding of the underlying bit-commitment scheme holds, we use $\mathcal{S}^*$ to construct an algorithm $M^{\mathcal{S}^*}$, described next, that violates the hardness of the universal one-way hash functions, $\mathcal{F}$. Recall that in order to violate the hardness of $\mathcal{F}$, $M^{\mathcal{S}^*}$ should succeed in the following experiment with non-negligible probability. $M^{\mathcal{S}^*}$ announces a value x and then given a random $f\in\mathcal{F}$, it needs to output $x'\neq x$ such that $f(x)=f(x')$.

Before presenting the algorithm, we would like first to make the dependency of $\mathcal{S}_c^*$ and $\mathcal{R}_c$ on the their random-coins explicit. That is, we assume that $\mathcal{S}_c^*$ and $\mathcal{R}_c$ are deterministic algorithms that get as additional inputs random strings $rand_{\mathcal{S}_c^*}\in\{0,1\}^{\ell_{\mathcal{S}_c^*}(n)}$ and $(phase,f,rand_{\mathcal{R}_c})\in\{\mathsf{first},\mathsf{second}\}\times\mathcal{F}\times\{0,1\}^{\ell_{\mathcal{R}_c}(n)}$ respectively. We assume w.l.o.g. that both $\ell_{\mathcal{S}_c^*}$ and $\ell_{\mathcal{R}_c}$ are some known polynomials.

$M^{\mathcal{S}^*}$**:**

First stage, announcing x.
Input: 1^n

a Select uniformly at random $rand=(rand_{\mathcal{S}_c^*},rand_{\mathcal{R}_c})\in\{0,1\}^{\ell_{\mathcal{S}_c^*}(n)}\times\{0,1\}^{\ell_{\mathcal{R}_c}(n)}$ and $f_1\in\mathcal{F}$.
b Simulate $\langle\mathcal{S}_c^*(rand_{\mathcal{S}_c^*}),\mathcal{R}_c(\mathsf{second},f_1,rand_{\mathcal{R}_c})\rangle$.
Let z be the value of 'z' that $\mathcal{S}_c^*$ sends to $\mathcal{R}_c$ in the above simulation.
c Output $x=z$ and $\mathsf{state}=rand$.

Second stage, finding a collision with x.
Input: $f_2\in\mathcal{F}$, $\mathsf{state}=(rand_{\mathcal{S}_c^*},rand_{\mathcal{R}_c})$, x.

d Simulate $\langle\mathcal{S}_c^*(rand_{\mathcal{S}_c^*}),\mathcal{R}_c(\mathsf{first},f_2,rand_{\mathcal{R}_c})\rangle$.
Let $\mathsf{outs}=(\mathsf{prvt},\mathsf{pub})$ be the private output of $\mathcal{S}_c^*$ and the public output in the above simulation.
e For both $i\in\{0,1\}$:
Simulate $\langle\mathcal{S}_r^*(\mathsf{prvt},\mathsf{pub},i),\mathcal{R}_r(\mathsf{pub},i)\rangle$.
Let z_i be the value of the variable 'z' that $\mathcal{S}_r^*$ sends to $\mathcal{R}_r$ in the above simulation.
f If there exists $j\in\{0,1\}$ such that $z_j\neq x$, then output it as x'.

Some intuition:.

By the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$, it follows that after the first-phase commit stage, there exists, at most, a single *value $\widetilde{z}$ (determined by the random coins of $\mathcal{S}^*$ and $\widetilde{\mathcal{R}}$) such that $\mathcal{S}^*$ is able to open the first-phase commitment to this value and then to cheat in the second-phase commitment.* [7] *Since we assume that $\mathcal{S}^*$ manages to cheat (also) for phase $=\mathsf{second}$, we therefore have that it must be able to break the binding second-phase commitment of $(\widetilde{\mathcal{S}},\widetilde{\mathcal{R}})$. Thus, it should hold that x, announced by $M^{\mathcal{S}^*}$, is equal to $\widetilde{z}$.*

Let us now consider the second-stage of $M^{\mathcal{S}^*}$. Since $\mathcal{S}_c^*$ does not know the value of phase when sending y in the

[7] We stress that information theoretically there might be many values that by opening the first-phase commitment to them, would allow cheating in the second-phase commitment. There is, however, at most one such value that $\mathcal{S}^*$ is able to open the commitment to it.

simulation of Line (d), it should send y such that $y = f_2(\widetilde{z})$ (where y is the value sent by $\mathcal{S}_r^*$ to $\mathcal{R}_r$ after the first-phase commit stage). The point is that since we are using the same random coins as in the first stage, this is the same $\widetilde{z}$ as before. Whenever $\mathcal{S}^*$ breaks the commitment for phase = first, it needs to send two distinct elements $z_0 \neq z_1$ such that $f_2(z_0) = f_2(z_1) = y$. Thus, w.h.p. it holds that $f_2(z_0) = f_2(z_1) = f_2(\widetilde{z}) = f_2(x)$ and $M^{\mathcal{S}^*}$ violates the hardness of $\mathcal{F}$.

CLAIM 3.7. *If $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is $\binom{2}{1}$-binding and Claim 3.6 does not hold, then $M^{\mathcal{S}^*}$ violates the hardness of $\mathcal{F}$.*

PROOF. For $rand \in rand_{\mathcal{S}_c^*} \times rand_{\mathcal{R}_c}$, $f \in \mathcal{F}$ and $phase \in \{\mathsf{first}, \mathsf{second}\}$, let $\mathsf{outs}(rand, f, phase)$ be the private and public outputs in the interaction of $\langle \mathcal{S}_c^*(rand_{\mathcal{S}_c^*}), \mathcal{R}_c(phase, f, rand_{\mathcal{R}_c})\rangle$. Similarly, let $z_c(rand, f)$ be the value of z that $\mathcal{S}_c^*$ sends to $\mathcal{R}_c$ in the interaction of $\langle \mathcal{S}_c^*(rand_{\mathcal{S}_c^*}), \mathcal{R}_c(\mathsf{second}, f, rand_{\mathcal{R}_c})\rangle$. Informally, the following lemma states that (the random coins of) the first-phase commitment determines a value $\widetilde{z}$ (and thus $\widetilde{z}$ is independent of f) such that the following hold: In case $phase = \mathsf{first}$, $\mathcal{S}^*$ finds a collision of $\widetilde{z}$ w.r.t. f. In case $phase = \mathsf{second}$, $\mathcal{S}^*$ opens the first-phase commitment to $\widetilde{z}$.

LEMMA 3.8 (MAPPING LEMMA). *Assuming that $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$ is $\binom{2}{1}$-binding and that Claim 3.6 does not hold, then there exists a set $L \subseteq \{0,1\}^{\ell_{\mathcal{S}_c^*}(n)} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$ of density $\frac{1}{6}$ and a mapping $\sigma : L \mapsto \{0,1\}^{\ell(n)}$ such that the following hold for all $rand \in L$:*

1. $\Pr_{f \leftarrow \mathcal{F}}[z_c(rand, f) = \sigma(rand)] \geq \frac{1}{2}$.
2. *For both values of $phase \in \{\mathsf{first}, \mathsf{second}\}$,* $\Pr_{f \leftarrow \mathcal{F}}[\mathsf{BindBreak}(\mathsf{outs}(rand, f, phase)) \geq \frac{1}{p(n)}] \geq \frac{5}{6}$.

We defer the proof of Lemma 3.8 and first use it for proving Claim 3.7. For $rand = (rand_{\mathcal{S}_c^*}, rand_{\mathcal{R}_c})$ and $f \in \mathcal{F}$, let $y(rand, f)$ be the value of y that $\mathcal{S}_c^*$ sends to $\mathcal{R}_c$ in the interaction of $\langle \mathcal{S}_c^*(rand_{\mathcal{S}_c^*}), \mathcal{R}_c(phase, f, rand_{\mathcal{R}_c})\rangle$ for some value of $phase$. (Note that $y(rand, f)$ is well defined, since y is sent before $phase$ is made public and thus it depends only on the values of $rand$ and f). For $i \in \{0,1\}$, we define the random variable $Z_r^i(rand, f)$ as the value of z that $\mathcal{S}_r^*$ sends to $\mathcal{R}_r$ in the (*reveal-stage*) interaction of $\langle \mathcal{S}_r^*(i, \mathsf{prvt}, \mathsf{pub}), \mathcal{R}_r(i, \mathsf{pub})\rangle$, where $(\mathsf{prvt}, \mathsf{pub}) = \mathsf{outs}(rand, f, \mathsf{first})$.

By the definition of $(\mathcal{S}, \mathcal{R})$ it follows that if $\mathcal{R}_r$ accepts in the interaction of $\langle \mathcal{S}_r^*(i, \mathsf{prvt}, \mathsf{pub}), \mathcal{R}_r(i, \mathsf{pub})\rangle$, it must hold that $f(Z_r^i(rand, f)) = y(rand, f)$ and that $h(Z_r^i(rand, f)) \oplus i = c$ (where h and c are the value of these variables that $\mathcal{S}_r^*$ sends to $\mathcal{R}_r$ in the interaction). It follows that if $\mathsf{BindBreak}(\mathsf{outs}(rand, \mathsf{first}, f)) \geq \varepsilon$ (for some $\varepsilon > 0$), then $\Pr[Z_r^0(rand, f) \neq Z_r^1(rand, f) \bigwedge f(Z_r^0(rand, f)) = Z_r^1(rand, f) = y(rand, f)] \geq \varepsilon^2$. On the other hand, if $\mathsf{BindBreak}(\mathsf{outs}(rand, \mathsf{second}, f)) > 0$, then it must hold that $f(z_c(rand, f)) = y(rand, f)$.

We conclude that if $\mathsf{BindBreak}(\mathsf{outs}(rand, phase, f)) \geq \varepsilon$ for both values of $phase$, then $\Pr[Z_r^0(rand, f) \neq Z_r^1(rand, f) \bigwedge f(Z_r^0(rand, f)) = Z_r^1(rand, f) = f(z_c(rand, f)))] \geq \varepsilon^2$. Thus, by applying Lemma 3.8 we have that for any $rand \in L$,

$$\Pr_{f \leftarrow \mathcal{F}}[Z_r^0(rand, f) \neq Z_r^1(rand, f) \bigwedge f(Z_r^0(rand, f)) = f(Z_r^1(rand, f)) = f(\sigma(rand))] \geq \frac{1}{p(n)^2} \cdot \Pr_{f \leftarrow \mathcal{F}}\Big[z_c(rand, f) = \sigma(rand) \bigwedge \forall phase \in \{\mathsf{first}, \mathsf{second}\} \ \mathsf{BindBreak}(\mathsf{outs}(rand, f, phase)) \geq \frac{1}{p(n)}\Big] \geq \frac{1}{p(n)^2} \cdot (\frac{1}{2} - \frac{1}{6} - \frac{1}{6}) = \frac{1}{6p(n)^2}, \quad (1)$$

where the probability is also over the random coins of $\mathcal{S}_r^*$.

We are now finally ready to show that $M^{\mathcal{S}^*}$ violates the hardness of $\mathcal{F}$. Recall the definition x, x', z_0 and z_1 from the definition of $M^{\mathcal{S}^*}$. By Eq. (1) it follows that conditioned on $\mathsf{state} \in L$,

$$\Pr_{f_2 \leftarrow \mathcal{F}}[z_0 \neq z_1 \bigwedge f_2(z_0) = f_2(z_1) = f(\sigma(\mathsf{state}))] \geq \frac{1}{6p(n)^2}. \quad (2)$$

Recall that x is defined as $z_c(\mathsf{state}, f_1)$. Thus, the first property of Lemma 3.8 yields that conditioned on $\mathsf{state} \in L$,

$$\Pr_{f_1 \leftarrow \mathcal{F}}[x = \sigma(\mathsf{state})] \geq \tfrac{1}{2}. \quad (3)$$

Conditioning on state, the events of Eq. (2) and Eq. (3) are independent. Hence, $\Pr[z_0 \neq z_1 \bigwedge f(x) = f(z_0) = f(z_1) \mid \mathsf{state} \in L] \geq \frac{1}{2} \cdot \frac{1}{6p(n)^2}$. Recall that x' takes the value in $\{z_0, z_1\}$ that is different than x. It follows that $\Pr[x' \neq x \bigwedge f_2(x') = f_2(x) \mid \mathsf{state} \in L] \geq \frac{1}{12p(n)^2}$ and since L is of noticeable density, $M^{\mathcal{S}^*}$ violates the hardness of $\mathcal{F}$.

PROOF. (of Lemma 3.8) For both $d \in \{\mathsf{first}, \mathsf{second}\}$, let G_d be the set of random coins that conditioned on $phase = d$, algorithm $\mathcal{S}^*$ manages to break the binding of the protocol with high probability. Namely, $G_d \stackrel{\text{def}}{=} \Big\{rand : \Pr_{f \leftarrow \mathcal{F}}[\mathsf{BindBreak}(\mathsf{outs}(rand, f, d)) \geq \frac{1}{p(n)}] \geq \frac{5}{6}\Big\}$. Since for both $d \in \{\mathsf{first}, \mathsf{second}\}$ we assumed that $\gamma_d^p(n) \geq \frac{17}{18}$, it follows by a straight forward averaging argument that for both $d \in \{\mathsf{first}, \mathsf{second}\}$ it holds that $\Pr[G_d] \geq \frac{2}{3}$. Therefore, $G \stackrel{\text{def}}{=} G_{\mathsf{first}} \cap G_{\mathsf{second}}$ is of density at least $\frac{1}{3}$. For any $z \in \{0,1\}^{\ell(n)}$ and any value of $rand$, let $w^{rand}(z) \stackrel{\text{def}}{=} \Pr_{f \leftarrow \mathcal{F}}[z_c(rand, f) = z]$.

CLAIM 3.9. $\Pr_{rand \leftarrow G}[\nexists z \in \{0,1\}^{\ell(n)} \ s.t. \ w^{rand}(z) > \frac{1}{2}] = neg$.

Thus, we conclude the proof of Lemma 3.8, by defining $L \stackrel{\text{def}}{=} G \cap \Big\{rand : \exists z \in \{0,1\}^{\ell(n)} \text{ s.t. } w^{rand}(z) > \frac{1}{2}\Big\}$ and defining $\sigma(rand)$ to be the value of $z \in \{0,1\}^{\ell(n)}$ for which $w^{rand}(z) > \frac{1}{2}$.

PROOF. (of Claim 3.9) For $rand = (rand_{\mathcal{S}_c^*}, rand_{\mathcal{R}_c})$ and $f \in \mathcal{F}$, let $\mathsf{trans}(rand, f, \mathsf{second})$ be the first-phase transcript of the interaction with $\widetilde{\mathcal{R}}$ embedded in the transcript of $\langle \mathcal{S}_c^*(rand_{\mathcal{S}_c^*}), \mathcal{R}_c(\mathsf{second}, f, rand_{\mathcal{R}_c})\rangle$ (i.e., the transcripts of the interactions with $\widetilde{\mathcal{R}}_c^1$ and $\widetilde{\mathcal{R}}_r^1$). Recall the set $\mathcal{B}$ from Definition 2.10 w.r.t. $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$, which has the property that if a first-phase transcript of an interaction with $\widetilde{\mathcal{R}}$ is in $\mathcal{B}$, then the second-phase commitment with $\widetilde{\mathcal{R}}$ is statistically binding. It follows that for almost all $rand \in G$ (save but a set of negligible probability) it holds that,

$$\Pr_{f \leftarrow \mathcal{F}}\Big[\mathsf{BindBreak}(\mathsf{outs}(rand, f, \mathsf{second})) \geq \frac{1}{p(n)} \bigwedge \mathsf{trans}(rand, f, \mathsf{second}) \notin \mathcal{B}\Big] \geq \frac{5}{6} - neg(n).$$

Let's assume towards a contradiction that Claim 3.9 does not hold. Therefore, by the above observation there exists a set $G' \subseteq G$ of non-negligible density such that the following holds for any $rand \in G'$:

1. $\nexists z \in \{0,1\}^{\ell(n)}$ s.t. $w^{rand}(z) > \frac{1}{2}$,
2. $\Pr_{f \leftarrow \mathcal{F}}\Big[\mathsf{BindBreak}(\mathsf{outs}(rand, f, \mathsf{second}) \geq \frac{1}{p(n)} \bigwedge \mathsf{trans}(rand, f, \mathsf{second}) \notin \mathcal{B}\Big] \geq \frac{2}{3}$.

We conclude the proof by showing that the existence of G' implies a violation of the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$. Before doing that, we would like to make the dependence of $\mathcal{R}_c$ in its random coins even more explicit. Recall that we assume that $\mathcal{R}_c$ is a deterministic algorithm that gets as an additional input the random coins $(phase, f, rand_{\mathcal{R}_c}) \in \{\mathsf{first}, \mathsf{second}\} \times \mathcal{F} \times \{0,1\}^{\ell_{\mathcal{R}_c}(n)}$. To make the discussion more precise, we write that $rand_{\mathcal{R}_c} = (rand_{\widetilde{\mathcal{R}}_c^1}, rand_{other})$ where $rand_{\widetilde{\mathcal{R}}_c^1} \in \{0,1\}^{\ell_{\widetilde{\mathcal{R}}_c^1}(n)}$ are the random coins used in the interaction of $\widetilde{\mathcal{R}}_c^1$ embedded in the interaction of $\mathcal{R}_c$. The following algorithm violates the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$.

$T^{\mathcal{S}^*}$**:**

Input: 1^n

The interaction part.

a Select uniformly at random $rand_{\mathcal{S}_c^*} \in \{0,1\}^{\ell_{\mathcal{S}_c^*}(n)}$.

b Interact with $\widetilde{\mathcal{R}}_c^1(1^n)$ by invoking $\mathcal{S}_c^*(rand_{\mathcal{S}_c^*})$ and simulating its interaction with $\mathcal{R}_c$ by forwarding messages between $\mathcal{S}_c^*$ and $\widetilde{\mathcal{R}}_c^1$.

Let trans^1 be the transcript of the above interaction and let $rand_{\widetilde{\mathcal{R}}_c^1}$ be the random coins used by $\widetilde{\mathcal{R}}_c^1$ in the above interaction. (We do not need to actually know the value of $rand_{\widetilde{\mathcal{R}}_c^1}$ for the run of $T^{\mathcal{S}^*}$ and only use it in order to simplify notation.)

Producing two transcripts.

a Select uniformly at random $rand_{other} \in \{0,1\}^{\ell_{\mathcal{R}_c^1}(n) - \ell_{\widetilde{\mathcal{R}}_c^1}(n)}$.

b For both $i \in \{0,1\}$:

1. Select uniformly at random $f_i \in \mathcal{F}$.
2. Simulate $\langle \mathcal{S}_c^*(rand_{\mathcal{S}_c^*}), \mathcal{R}_c(\mathsf{second}, f_i, rand_{\widetilde{\mathcal{R}}_c}, rand_{other}) \rangle$ starting from Line 3 of Construction 3.1. (Note that given trans^1, we do not need to know $rand_{\widetilde{\mathcal{R}}_c}$ in order to simulate).

   Let $\mathsf{outs}_i^2 = (\mathsf{prvt}_i^2, \mathsf{pub}_i^2)$, where prvt_i^2 and prvt_i^2 are the private output of $\mathcal{S}_c^*$ and the public output in the above simulation respectively. Let trans_i^2 and trans_i^3 be the transcripts of the interactions with $\widetilde{\mathcal{R}}_r^1$ and $\widetilde{\mathcal{R}}_c^2$ in the above simulation.
3. Simulate $\langle \mathcal{S}_r^*(\mathsf{prvt}_i^2, \mathsf{pub}_i^2, 0), \mathcal{R}_r(\mathsf{pub}_i^2, 0) \rangle$. Let trans_i^4 be the transcript of the interaction with $\widetilde{\mathcal{R}}_r^2$ in the above simulation.
4. Set $\mathsf{trans}_i = (\mathsf{trans}^1, \mathsf{trans}_i^2, \mathsf{trans}_i^3, \mathsf{trans}_i^4)$.

c Output $(\mathsf{trans}_0, \mathsf{trans}_1)$.

CLAIM 3.10. *$T^{\mathcal{S}^*}$ violates the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$.*

PROOF. Conditioned on $rand \in G'$, we have by the second property of G' that

$$\Pr_{f_0 \leftarrow \mathcal{F}}\left[\mathsf{BindBreak}(\mathsf{outs}_0) \geq \frac{1}{p(n)} \bigwedge (\mathsf{trans}^1, \mathsf{trans}_0^2) \notin \mathcal{B}\right] \geq \frac{2}{3}. \tag{4}$$

Clearly, the above also holds w.r.t. f_1, outs_1 and trans_1^2. Moreover, by the first property of G', we have the following w.r.t. any $z \in \{0,1\}^{\ell(n)}$,

$$\Pr_{f_1 \leftarrow \mathcal{F}}[z_c(rand, f_1) \neq z \bigwedge \mathsf{BindBreak}(\mathsf{outs}_1) \geq \frac{1}{p(n)} \bigwedge (\mathsf{trans}^1, \mathsf{trans}_1^2) \notin \mathcal{B}] \geq \frac{2}{3} - \frac{1}{2} = \frac{1}{6}. \tag{5}$$

Setting $z = z_c(rand, f_1)$, since f_1 is independent of f_0, it follows that

$$\begin{aligned} &\Pr_{f_0 \leftarrow \mathcal{F}, f_1 \leftarrow \mathcal{F}}\Big[z_c(rand, f_0) \neq z_c(rand, f_1) \bigwedge \forall i \in \{0,1\} \\ &\quad \mathsf{BindBreak}(\mathsf{outs}_i) \geq \frac{1}{p(n)} \bigwedge (\mathsf{trans}^1, \mathsf{trans}_i^2) \notin \mathcal{B}\Big] \\ \geq\ & \frac{2}{3} \cdot \frac{1}{6} = \frac{1}{9}. \end{aligned}$$

Therefore, we conclude that condition that $rand \in G'$, the following happens with probability at least $\frac{1}{9} \cdot \frac{1}{p(n)^2}$:

1. both trans_0 and trans_1 starts with trans^1,
2. the first-phase transcripts (i.e., $(\mathsf{trans}^1, \mathsf{trans}_i^2)$) in both trans_0 and trans_1 are not in $\mathcal{B}$,
3. the value of z in trans_0 and in trans_1 is different,
4. $\widetilde{\mathcal{R}}_r^1$ and $\widetilde{\mathcal{R}}_r^2$ accept in both trans_0 and trans_1.

Since we assume that the density of G' is non-negligible, $T^{\mathcal{S}^*}$ violates the $\binom{2}{1}$-binding of $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{R}})$. □

Thus, we have concluded the proof of Lemma 3.8 and hence the proof of Lemma 3.5.

3.2 Completing the construction

The following corollary follows by the lemmata about Construction 3.1 (Lemma 3.1 and Lemma 3.5) and the standard bit-commitment binding amplification (Proposition 2.9).

COROLLARY 3.11. *There exists an efficient procedure that given a two-phase commitment scheme and a family of universal one-way hash functions, outputs a bit-commitment scheme which is statistically hiding whenever the underlying protocol is statistically hiding and is computationally binding whenever the underlying protocol is* $\binom{2}{1}$*-binding.*

As the existence of one-way functions implies the existence of universal one-way hash functions of the appropriate input and output lengths (Theorem 2.4) and of a collections of two-phase commitment schemes (for any choice of message lengths) that are all $\binom{2}{1}$-binding and at least one of them is statistically hiding (Theorem 2.13 and Remark 2.14). We have by the above Corollary and the standard bit-commitment hiding amplification (Proposition 2.8), that statistical bit-commitment can be constructed using any one-way function. Finally, the proof of Theorem 1.1 follows by the above conclusion and the standard transformation of a bit-commitment scheme into a commitment scheme of any polynomial length.

REMARK 3.12. *Note that since the reveal stage of the commitments guaranteed by Theorem 2.13 are non interactive (i.e., consistent on a single message from the sender to the receiver), the reveal stage of our commitment scheme is non-interactive as well.*

Acknowledgments

We are grateful to Danny Harnik, Oded Goldreich, Tal Moran, Moni Naor, Alon Rosen and Salil Vadhan for very helpful conversations. We are also grateful to Claude Crépeau, Adam Smith and to the anonymous referees for their useful comments.

4. REFERENCES

[1] J. Boyar, S. Kurtz, and M. Krentel. Discrete logarithm implementation of perfect zero-knowledge blobs. *JCRYPTOLOGY*, 1990.

[2] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *JCSS*, 1988.

[3] J. Carter and M. Wegman. Universal classes of hash functions. *JCSS*, 1979.

[4] I. Damgard, M. Pedersen, and B. Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *JCRYPTOLOGY*, 1997.

[5] O. Goldreich. Randomized methods in computation - lecture notes. 2001.

[6] O. Goldreich and A. Kahan. How to construct constant-round zero-knowledge proof systems for NP. *JCRYPTOLOGY*, 1996.

[7] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. on Computing*, 1988.

[8] I. Haitner, O. Horvitz, K. J, C. Koo, R. Morselli, and R. Shaltiel. Reducing complexity assumptions for statistically-hiding commitment. In *EUROCRYPT*, 2005.

[9] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal of Computing*, 1999.

[10] R. Impagliazzo and M. Luby. One-way functions are essential for complexity-based cryptography. In *30 FOCS*, 1989.

[11] J. Katz and C. Koo. On constructing universal one-way hash functions from arbitrary one-way functions. ePrint, Report 2005/328, 2005.

[12] Y. Lindell. Parallel coin-tossing and constant-round secure two-party computation. *JCRYPTOLOGY*, 2003.

[13] M. Naor. Bit commitment using pseudorandomness. *JCRYPTOLOGY*, 1991.

[14] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung. Perfect zero-knowledge arguments for NP using any one-way permutation. *JCRYPTOLOGY*, 1998.

[15] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic application. In *21st STOC*, 1989.

[16] M. Nguyen, S. Ong, and S. Vadhan. Statistical zero-knowledge arguments for NP from any one-way function. In *39th FOCS*, 2006.

[17] M. Nguyen and S. Vadhan. Zero knowledge with efficient provers. In *38th STOC*, 2006.

[18] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd STOC*, 1990.